SYSTEM AND METHOD FOR SERVER SIDE DATA SIGNING

Abstract of the Disclosure

To ensure data integrity, data are signed using a server-side key before being stored with a signature in a persistent storage on a client. Before the data that were stored are subsequently used, the data signature is verified to confirm that the data have not been modified. A signer identification (ID) uniquely identifying the client is sealed into the signature so that the identity of the signer cannot be changed without invalidating the data signature. If the data or the signer ID is altered, a temporary signature computed for the stored data and signer ID will differ from the signature that was stored. The server preferably signs a digest of the data to be stored and verifies a digest of the stored data. An intermediate key can be provided by the server to enable plural sets of data on the client to be signed before storage.